

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2020年1月2日(02.01.2020)



(10) 国際公開番号

WO 2020/003406 A1

(51) 国際特許分類:
G06F 13/00 (2006.01)

(21) 国際出願番号: PCT/JP2018/024373

(22) 国際出願日: 2018年6月27日(27.06.2018)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人:三菱電機株式会社(MITSUBISHI ELECTRIC CORPORATION) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目7番3号 Tokyo (JP).

(72) 発明者: 西川 弘毅 (NISHIKAWA, Hiroki); 〒1008310 東京都千代田区丸の内二丁目7番3号 三菱電機株式会社内 Tokyo (JP). 山本匠 (YAMAMOTO, Takumi); 〒1008310 東京都千代田区丸の内二丁目7番3号 三菱電機株式会社内 Tokyo (JP). 河内 清人(KAWAUCHI,

Kiyoto); 〒1008310 東京都千代田区丸の内二丁目7番3号 三菱電機株式会社内 Tokyo (JP).

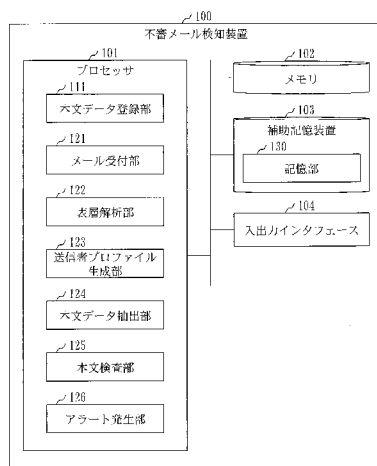
(74) 代理人: 溝井 国際特許業務法人(MIZOI INTERNATIONAL PATENT FIRM); 〒2470056 神奈川県鎌倉市大船二丁目17番10号3階 Kanagawa (JP).

(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(54) Title: SUSPICIOUS MAIL DETECTION DEVICE, SUSPICIOUS MAIL DETECTION METHOD, AND SUSPICIOUS MAIL DETECTION PROGRAM

(54) 発明の名称: 不審メール検知装置、不審メール検知方法および不審メール検知プログラム

[図1]



100 Suspicious mail detection device
101 Processor
102 Memory
103 Auxiliary storage device
104 Input and output interface
111 Body text data registration unit
121 Mail reception unit
122 Surface layer analysis unit
123 Sender profile generation unit
124 Body text data extraction unit
125 Body text inspection unit
126 Alert generation unit
130 Storage unit

(57) Abstract: A sender profile generation unit (123) generates a sender profile of a subject mail on the basis of the subject mail, which is an e-mail to be inspected. A body text data extraction unit (124) extracts body text data corresponding to the sender profile of the subject mail from a body text list file in which one or more pieces of body text data relating to one or more suspicious mails and one or more sender profiles relating to the one or more suspicious mails are associated with each other. A body text inspection unit (125) compares a body text of the subject mail with the body text data extracted from the body text list file, and determines whether the subject mail is a suspicious mail or not on the basis of a result of the comparison.

(57) 要約: 送信者プロフィール生成部(123)は、検査対象の電子メールである対象メールに基づいて前記対象メールの送信者プロフィールを生成する。本文データ抽出部(124)は、1つ以上の不審メールについての1つ以上の本文データと、前記1つ以上の不審メールについての1つ以上の送信者プロフィールと、が互いに対応付けられた本文一覧ファイルから、前記対象メールの前記送信者プロフィールに対応する本文データを抽出する。本文検査部(125)は、前記対象メールの本文を前記本文一覧ファイルから抽出された本文データと比較し、比較結果に基づいて前記対象メールが不審メールであるか判定する。

[続葉有]

(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類：

一 国際調査報告 (条約第21条(3))

明 細 書

発明の名称：

不審メール検知装置、不審メール検知方法および不審メール検知プログラム

技術分野

[0001] 本発明は、不審な電子メールを検知するための技術に関するものである。

背景技術

[0002] 標的型攻撃が深刻な脅威となっている。標的型攻撃は、特定の組織または特定の人を対象として、機密情報の窃取等を目的とする攻撃である。

標的型攻撃の中でも、標的型メール攻撃は、依然として重大な脅威の一つである。標的型メール攻撃は、電子メールをベースにした攻撃である。

トレンドマイクロの調査では、標的型メール攻撃によるマルウェア感染は企業に対する攻撃全体の76パーセントにも上る、との結果が出ている。そのため、標的型メール攻撃を防ぐことは、被害を増加させる巧妙なサイバー攻撃を防ぐ観点から重要である。

このような背景の元、標的型攻撃メールを検知することによって標的型メール攻撃から組織を防ぐための技術が検討されている。

[0003] 特許文献1には、受信メールのヘッダを学習済みの正規ヘッダと比較することによって、受信メールが不審な電子メールであるか判断する技術が開示されている。

特許文献2には、電子メールに添付されるファイルが不審であるか判断するためにファイルのフォーマットを特定し、特定したフォーマットが許可されるものであるか判定する技術が開示されている。

特許文献3には、新規メールのヘッダ情報と過去メールのヘッダ情報との類似度が低い場合に新規メールが不審な電子メールであると判断する技術が開示されている。

特許文献4には、受信メールの本文とスパムメッセージの本文との類似度

が閾値を超える場合に受信メールが不審な電子メールであると判断する技術が開示されている。

[0004] 非特許文献1および非特許文献2については、実施の形態において言及する。

先行技術文献

特許文献

[0005] 特許文献1：特開2013-236308号公報

特許文献2：特表2008-546111号公報

特許文献3：特開2014-102708号公報

特許文献4：特表2007-503660号公報

非特許文献

[0006] 非特許文献1：Mikolov, Tomas, et al. “Efficient estimation of word representations in vector space.”, arXiv preprint arXiv:1301.3781 (2013)

非特許文献2：岡野裕樹、木邑実、辻宏郷、青木眞夫，“IPAテクニカルウォッチ「標的型攻撃メールの見分け方」”，独立行政法人情報処理推進機構 技術本部 セキュリティセンター，2015年1月9日

発明の概要

発明が解決しようとする課題

[0007] 特許文献1または特許文献3に開示された技術のように電子メールのヘッダに基づいて電子メールが不審であるか判定する方法では、メールヘッダが正規のヘッダであるように偽装された電子メールを検知することができない。

特許文献2に開示された技術のように添付ファイルのフォーマットに基づいて添付ファイルが不審であるか判定する方法では、中身が不正であるがフォーマットが正しい電子メールを検知することができない。

特許文献４に開示された技術のように電子メールの本文とスパムメッセージの本文との類似度に基づいて電子メールが不審であるか判定する方法では、電子メールの本文と比較するスパムメッセージの本文が適切なものでなければ電子メールが不審であるか適切に判定することができない。また、電子メールの本文をあらゆるスパムメッセージの本文と比較しようとすると、処理負荷および処理時間が増大してしまう。

[0008] 本発明は、電子メールが不審であるか適切に判定できるようにすることを目的とする。

課題を解決するための手段

[0009] 本発明の不審メール検知装置は、
検査対象の電子メールである対象メールに基づいて前記対象メールの送信者プロフィールを生成する送信者プロフィール生成部と、
１つ以上の不審メールについての１つ以上の本文データと、前記１つ以上の不審メールについての１つ以上の送信者プロフィールと、が互いに対応付けられた本文一覧ファイルから、前記対象メールの前記送信者プロフィールに対応する本文データを抽出する本文データ抽出部と、
前記対象メールの本文を前記本文一覧ファイルから抽出された本文データと比較し、比較結果に基づいて前記対象メールが不審メールであるか判定する本文検査部とを備える。

発明の効果

[0010] 本発明によれば、電子メールの本文を電子メールの本文と比較する不審メールの本文として適切なものと比較し、比較結果に基づいて電子メールが不審であるか判定することが可能となる。そのため、電子メールが不審であるか適切に判定することが可能となる。

図面の簡単な説明

[0011] [図1]実施の形態１における不審メール検知装置１００の構成図。

[図2]実施の形態１における不審メール検知方法の概要図。

[図3]実施の形態１における不審メール検知方法のフローチャート。

[図4]実施の形態1における本文一覧ファイル131Aを示す図。

[図5]実施の形態1における本文一覧ファイル131Bを示す図。

[図6]実施の形態1における運用フェーズ(S120)のフローチャート。

[図7]実施の形態1における本文検査処理(S126)のフローチャート。

[図8]実施の形態1における不審メール検知装置100のハードウェア構成図。
。

発明を実施するための形態

[0012] 実施の形態および図面において、同じ要素または対応する要素には同じ符号を付している。説明した要素と同じ符号が付された要素の説明は適宜に省略または簡略化する。図中の矢印はデータの流れ又は処理の流れを主に示している。

[0013] 実施の形態1.

不審な電子メールを検知する形態について、図1から図7に基づいて説明する。

[0014] ***構成の説明***

図1に基づいて、不審メール検知装置100の構成を説明する。

不審メール検知装置100は、プロセッサ101とメモリ102と補助記憶装置103と入出力インタフェース104といったハードウェアを備えるコンピュータである。これらのハードウェアは、信号線を介して互いに接続されている。

[0015] プロセッサ101は、演算処理を行うIC(Integrated Circuit)であり、他のハードウェアを制御する。例えば、プロセッサ101は、CPU(Central Processing Unit)、DSP(Digital Signal Processor)、またはGPU(Graphics Processing Unit)である。

メモリ102は揮発性の記憶装置である。メモリ102は、主記憶装置またはメインメモリとも呼ばれる。例えば、メモリ102はRAM(Random Access Memory)である。メモリ102に記憶されたデ

ータは必要に応じて補助記憶装置１０３に保存される。

補助記憶装置１０３は不揮発性の記憶装置である。例えば、補助記憶装置１０３は、ROM (Read Only Memory)、HDD (Hard Disk Drive)、またはフラッシュメモリである。補助記憶装置１０３に記憶されたデータは必要に応じてメモリ１０２にロードされる。

入出力インタフェース１０４は入力装置および出力装置が接続されるポートである。例えば、入出力インタフェース１０４はUSB端子であり、入力装置はキーボードおよびマウスであり、出力装置はディスプレイである。USBはUniversal Serial Busの略称である。

[0016] 不審メール検知装置１００は、本文データ登録部１１１とメール受付部１２１と表層解析部１２２と送信者プロフィール生成部１２３と本文データ抽出部１２４と本文検査部１２５とアラート発生部１２６といった要素を備える。これらの要素はソフトウェアで実現される。

[0017] 補助記憶装置１０３には、本文データ登録部１１１とメール受付部１２１と表層解析部１２２と送信者プロフィール生成部１２３と本文データ抽出部１２４と本文検査部１２５とアラート発生部１２６としてコンピュータを機能させるための不審メール検知プログラムが記憶されている。不審メール検知プログラムは、メモリ１０２にロードされて、プロセッサ１０１によって実行される。

さらに、補助記憶装置１０３にはOS (Operating System) が記憶されている。OSの少なくとも一部は、メモリ１０２にロードされて、プロセッサ１０１によって実行される。

つまり、プロセッサ１０１は、OSを実行しながら、不審メール検知プログラムを実行する。

不審メール検知プログラムを実行して得られるデータは、メモリ１０２、補助記憶装置１０３、プロセッサ１０１内のレジスタ、または、プロセッサ１０１内のキャッシュメモリといった記憶装置に記憶される。

[0018] 補助記憶装置１０３は記憶部１３０として機能する。但し、他の記憶装置

が、補助記憶装置 103 の代わりに、又は、補助記憶装置 103 と共に、記憶部 130 として機能してもよい。

[0019] 不審メール検知装置 100 は、プロセッサ 101 を代替する複数のプロセッサを備えてもよい。複数のプロセッサは、プロセッサ 101 の役割を分担する。

[0020] 不審メール検知プログラムは、光ディスクまたはフラッシュメモリ等の不揮発性の記録媒体にコンピュータ読み取り可能に記録（格納）することができる。

[0021] ***動作の説明***

不審メール検知装置 100 の動作は不審メール検知方法に相当する。また、不審メール検知方法の手順は不審メール検知プログラムの手順に相当する。

[0022] 図 2 に基づいて、不審メール検知方法の概要を説明する。

メール受付部 121 は、検査対象の電子メールを受け取る。

検査対象の電子メールを対象メールという。

[0023] 表層解析部 122 は、対象メールに対する表層解析によって、対象メールが不審メールであるか判定する。

不審メールは、不審な電子メールである。例えば、不審メールは、標的型攻撃メールであると推測される電子メールである。標的型電子メールは、標的型メール攻撃を行うための電子メールである。

[0024] 表層解析部 122 によって対象メールが不審メールであると判定された場合、アラート発生部 126 はアラートを発生させる。

[0025] 送信者プロファイル生成部 123 は、対象メールに基づいて、対象メールの送信者プロファイルを生成する。

送信者プロファイルは、電子メールの送信者に関する情報を示すデータである。

[0026] 本文データ抽出部 124 は、本文一覧ファイルから、対象メールの送信者プロファイルに対応する本文データを抽出する。

本文一覧ファイルは、１つ以上の不審メールについての１つ以上の本文データと、前記１つ以上の不審メールについての１つ以上の送信者プロフィールと、が互いに対応付けられたファイルである。

本文データは、不審メールの本文の文面を表すデータである。

[0027] 本文検査部１２５は、対象メールの本文を本文一覧ファイルから抽出された本文データと比較する。そして、本文検査部１２５は、比較結果に基づいて、対象メールが不審メールであるか判定する。

具体的には、本文検査部１２５は、表層解析によって対象メールが不審メールであると判定されない場合に、対象メールが不審メールであるか判定する。

[0028] 本文検査部１２５によって対象メールが不審メールであると判定された場合、アラート発生部１２６はアラートを発生させる。

[0029] 図３に基づいて、不審メール検知方法の手順を説明する。

ステップＳ１１０は準備フェーズである。

ステップＳ１１０において、利用者は、１つ以上の不審メールのそれぞれについて本文データと送信者プロフィールとの組を不審メール検知装置１００に入力する。

本文データ登録部１１１は、１つ以上の不審メールのそれぞれについて本文データと送信者プロフィールとの組を受け付ける。そして、本文データ登録部１１１は、１つ以上の不審メールのそれぞれについて本文データと送信者プロフィールとの組を本文一覧ファイル１３１に登録する。本文一覧ファイル１３１は記憶部１３０に記憶される。

例えば、利用者は、情報処理に関する組織が公開する標的型攻撃メールの文面例を参考にすることによって、本文データと送信者プロフィールとの組を作成することが可能である。情報処理に関する組織の一例は、情報処理推進機構（ＩＰＡ）である。非特許文献２は、標的型攻撃メールの例と見分け方を示している。

[0030] 図４および図５に基づいて、本文一覧ファイル１３１を説明する。

図4の本文一覧ファイル131Aおよび図5の本文一覧ファイル131Bは、本文一覧ファイル131の具体例である。

本文一覧ファイル131Aおよび本文一覧ファイル131Bは、本文データと送信プロファイルとの組を2つ以上含んでいる。

[0031] 図4の本文一覧ファイル131Aにおいて、本文データは、不審メールの本文の文面を示している。

第1本文データにおいて、 X_1 は法人名を表し、 X_2 は大学名を表し、 X_3 は送信者名を表している。

第2本文データにおいて、 Y_1 は会社名を表し、 Y_2 はソフトウェア名を表している。

[0032] 図5の本文一覧ファイル131Bにおいて、本文データは、不審メールの本文についての文面のパターンを示している。

具体的には、本文データは、不審メールの本文で使用される1つ以上の語と1つ以上の語の順序とを示している。

[XXX]は、プレースホルダであり、「XXX」を識別する固有名詞を意味する。つまり、本文データにおいて、固有名詞はプレースホルダに置き換えられている。例えば、[組織名]は、組織名を識別する固有名詞を意味する。

さらに、動詞の活用等の問題を無視するために、原型だけを本文データに含めるようにするとよい。

[0033] 図4の本文一覧ファイル131Aおよび図5の本文一覧ファイル131Bにおいて、送信者プロファイルは、アドレスと所属と業界と属性といったプロファイル情報を含んでいる。

送信者プロファイルにおけるアドレスは、送信者のメールアドレスを示す。

送信者プロファイルにおける所属は、送信者が所属する団体を示す。

送信者プロファイルにおける業界は、送信者が所属する団体が属する業界を示す。

送信者プロフィールにおける属性は、送信者の属性またはメール本文の属性を示す。

第1本文データにおいて、 X_2 は大学名を表している。

第2本文データにおいて、 Y_3 は団体名を表している。

[0034] 送信者の名前および送信者のドメインもプロフィール情報の一例である。

プロフィール情報は辞書型であり、送信者名または所属などのラベルをキーとしてキーに対応付けてプロフィール情報が管理される。

[0035] 図3に戻り、ステップS120から説明を続ける。

ステップS120は運用フェーズである。

ステップS120において、不審メール検知装置100は、対象メールが不審メールであるか判定する。

[0036] 図6に基づいて、運用フェーズ（S120）の手順を説明する。

ステップS121において、メール受付部121は、検査対象となる電子メールを受け取る。受け取られる電子メールを対象メールという。

例えば、メール受付部121は、メールシステムから対象メールを受け取る。メールシステムの具体例は、メールサーバまたはメールクライアントである。

[0037] ステップS122において、表層解析部122は、対象メールに対する表層解析を行う。具体的には、表層解析部122は、対象メールのヘッダに対する表層解析を行う。

そして、表層解析部122は、解析結果に基づいて、対象メールが不審メールであるか判定する。

例えば、表層解析部122は、特許文献1から特許文献4のいずれかに開示されている方法で、対象メールが不審メールであるか判定する。

対象メールが不審メールである場合、処理はステップS123に進む。

対象メールが不審メールでない場合、処理はステップS124に進む。

[0038] ステップS123において、アラート発生部126は、アラートを発生させる。

例えば、アラート発生部 1 2 6 は、アラートメッセージをディスプレイに表示する。アラートメッセージは、不審な電子メール（対象メール）が発生したことを知らせる。

ステップ S 1 2 3 の後、運用フェーズ（S 1 2 0）は終了する。

[0039] ステップ S 1 2 4 において、送信者プロファイル生成部 1 2 3 は、対象メールの送信者プロファイルを生成する。

[0040] 例えば、送信者プロファイル生成部 1 2 3 は、対象メールの送信者プロファイルに含める情報を以下のように取得する。

送信者プロファイル生成部 1 2 3 は、対象メールのヘッダから、送信者のメールアドレスを抽出する。

送信者プロファイル生成部 1 2 3 は、対象メールの本文を解析することによって、対象メールの本文から、送信者が所属する団体の名称（所属名）を抽出する。

送信者プロファイル生成部 1 2 3 は、送信者の所属名をインターネットで検索する。そして、送信者プロファイル生成部 1 2 3 は、検索結果から得られる情報に基づいて、送信者が所属する団体が属する業界の名称（業界名）を判定する。

送信者プロファイル生成部 1 2 3 は、送信者の所属名に基づいて、送信者の属性を判定する。

送信者プロファイル生成部 1 2 3 は、対象メールの本文を解析することによって、対象メールの本文の属性を判定する。

[0041] ステップ S 1 2 5 において、本文データ抽出部 1 2 4 は、本文一覧ファイル 1 3 1 から、対象メールの送信者プロファイルに対応する 1 つ以上の本文データを抽出する。

[0042] 具体的には、本文データ抽出部 1 2 4 は、対象メールの送信者プロファイルに対応する本文データを以下のように抽出する。

まず、本文データ抽出部 1 2 4 は、対象メールの送信者プロファイルと合致する送信者プロファイルを本文一覧ファイル 1 3 1 から選択する。例えば

、対象メールの送信者プロフィールと合致する送信者プロフィールは、対象メールの送信者プロフィールに含まれる全ての情報を含んだ送信者プロフィールである。また例えば、対象メールの送信者プロフィールと合致する送信者プロフィールは、対象メールの送信者プロフィールとの合致度が閾値を超える送信者プロフィールである。対象メールの送信者プロフィールとの合致度は、対象メールの送信者プロフィールと共通する情報の数が多いほど高い。

そして、本文データ抽出部124は、選択した送信者プロフィールに対応付けられた本文データを本文一覧ファイル131から抽出する。抽出される本文データが、対象メールの送信者プロフィールに対応する本文データである。

[0043] ステップS126において、本文検査部125は、本文一覧ファイル131から抽出された1つ以上の本文データに基づいて、対象メールの本文を検査する。

ステップS126の後、運用フェーズ(S120)は終了する。

[0044] 図7に基づいて、本文検査処理(S126)の手順を説明する。

ステップS1261において、本文検査部125は、本文一覧ファイル131から抽出された1つ以上の本文データの中から、未選択の本文データを1つ選択する。

[0045] ステップS1262における本文データは、ステップS1261で選択された本文データである。

[0046] ステップS1262において、本文検査部125は、対象メールの本文を本文データと比較することによって、対象メールの本文と本文データとの類似度を算出する。対象メールの本文の文面が本文データによって表される文面に似ているほど、対象メールの本文と本文データとの類似度は高い。

[0047] 例えば、本文検査部125は、対象メールの本文と本文データとの類似度を以下のように算出する。

まず、本文検査部125は、対象メールの本文における文面の特徴ベクト

ル（対象特徴ベクトル）と、本文データによって表される文面の特徴ベクトル（比較特徴ベクトル）と、を既存技術によって算出する。既存技術の具体例はWord2Vecである。非特許文献1はWord2Vecに関する文献である。Word2Vecを応用することによって、電子メールの本文から分散表現を抽出し、抽出した分散表現を特徴ベクトルで表すことができる。

そして、本文検査部125は、対象特徴ベクトルと比較特徴ベクトルとのコサイン類似度を算出する。算出されるコサイン類似度が対象メールの本文と本文データとの類似度である。

[0048] ステップS1263において、本文検査部125は、ステップS1262で算出した類似度を閾値と比較する。

類似度が閾値以上である場合、処理はステップS1265に進む。

類似度が閾値未満である場合、処理はステップS1264に進む。

[0049] ステップS1264において、本文検査部125は、ステップS1261で選択されていない本文データが有るか判定する。ステップS1264において、ステップS1261で選択されていない本文データを未選択データという。

未選択データが有る場合、処理はステップS1261に進む。

未選択データが無い場合、本文検査処理（S126）は終了する。

[0050] ステップS1265において、アラート発生部126は、アラートを発生させる。

例えば、アラート発生部126は、アラートメッセージをディスプレイに表示する。アラートメッセージは、不審な電子メール（対象メール）が発生したことを知らせる。

ステップS1265の後、本文検査処理（S126）は終了する。

[0051] ***実施の形態1の効果***

ヘッダ等の表層情報が自然であっても悪意あるやり取りが実施された際に不審な電子メールを検知することができる。その結果、攻撃者による巧妙な

攻撃を防ぐことが可能となる。

[0052] ***実施の形態の補足***

図8に基づいて、不審メール検知装置100のハードウェア構成を説明する。

不審メール検知装置100は処理回路109を備える。

処理回路109は、本文データ登録部111とメール受付部121と表層解析部122と送信者プロファイル生成部123と本文データ抽出部124と本文検査部125とアラート発生部126とを実現するハードウェアである。

処理回路109は、専用のハードウェアであってもよいし、メモリ102に格納されるプログラムを実行するプロセッサ101であってもよい。

[0053] 処理回路109が専用のハードウェアである場合、処理回路109は、例えば、単回路、複合回路、プログラム化したプロセッサ、並列プログラム化したプロセッサ、ASIC、FPGAまたはこれらの組み合わせである。

ASICはApplication Specific Integrated Circuitの略称であり、FPGAはField Programmable Gate Arrayの略称である。

不審メール検知装置100は、処理回路109を代替する複数の処理回路を備えてもよい。複数の処理回路は、処理回路109の役割を分担する。

[0054] 処理回路109において、一部の機能が専用のハードウェアで実現されて、残りの機能がソフトウェアまたはファームウェアで実現されてもよい。

[0055] このように、処理回路109はハードウェア、ソフトウェア、ファームウェアまたはこれらの組み合わせで実現することができる。

[0056] 実施の形態は、好ましい形態の例示であり、本発明の技術的範囲を制限することを意図するものではない。実施の形態は、部分的に実施してもよいし、他の形態と組み合わせて実施してもよい。フローチャート等を用いて説明した手順は、適宜に変更してもよい。

符号の説明

[0057] 100 不審メール検知装置、101 プロセッサ、102 メモリ、103 補助記憶装置、104 入出力インタフェース、109 処理回路、111 本文データ登録部、121 メール受付部、122 表層解析部、123 送信者プロフィール生成部、124 本文データ抽出部、125 本文検査部、126 アラート発生部、130 記憶部、131 本文一覧ファイル。

請求の範囲

- [請求項1] 検査対象の電子メールである対象メールに基づいて前記対象メールの送信者プロフィールを生成する送信者プロフィール生成部と、
- 1つ以上の不審メールについての1つ以上の本文データと、前記1つ以上の不審メールについての1つ以上の送信者プロフィールと、が互いに対応付けられた本文一覧ファイルから、前記対象メールの前記送信者プロフィールに対応する本文データを抽出する本文データ抽出部と、
- 前記対象メールの本文を前記本文一覧ファイルから抽出された本文データと比較し、比較結果に基づいて前記対象メールが不審メールであるか判定する本文検査部と
- を備える不審メール検知装置。
- [請求項2] 前記不審メール検知装置は、さらに、
- 前記対象メールに対する表層解析によって前記対象メールが不審メールであるか判定する表層解析部
- を備える請求項1に記載の不審メール検知装置。
- [請求項3] 前記本文検査部は、前記表層解析によって前記対象メールが不審メールであると判定されない場合に、前記対象メールが不審メールであるか判定する
- 請求項2に記載の不審メール検知装置。
- [請求項4] 送信者プロフィール生成部が、検査対象の電子メールである対象メールに基づいて前記対象メールの送信者プロフィールを生成し、
- 本文データ抽出部が、1つ以上の不審メールについての1つ以上の本文データと、前記1つ以上の不審メールについての1つ以上の送信者プロフィールと、が互いに対応付けられた本文一覧ファイルから、前記対象メールの前記送信者プロフィールに対応する本文データを抽出し、
- 本文検査部が、前記対象メールの本文を前記本文一覧ファイルから

抽出された本文データと比較し、比較結果に基づいて前記対象メールが不審メールであるか判定する

不審メール検知方法。

[請求項5]

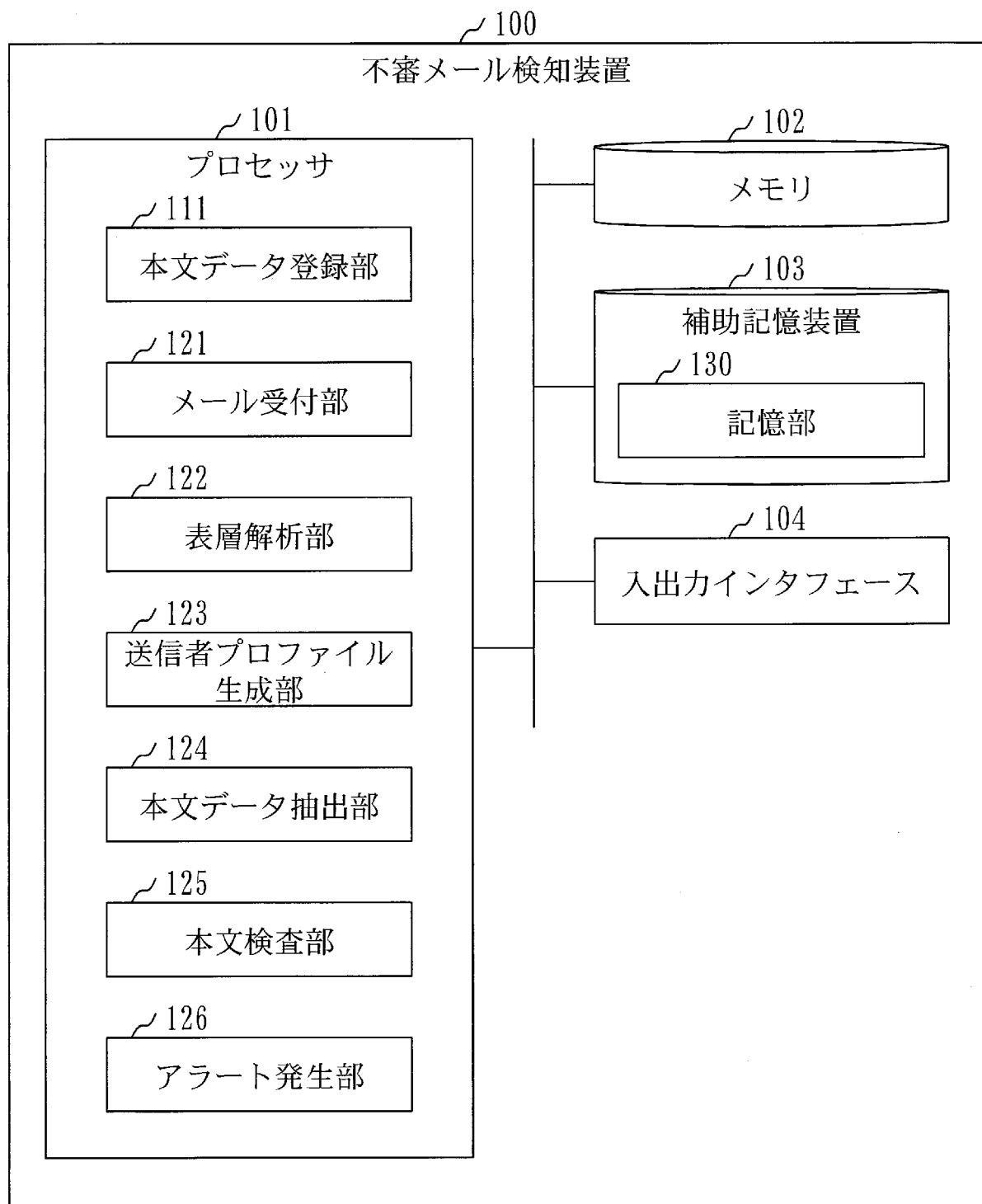
検査対象の電子メールである対象メールに基づいて前記対象メールの送信者プロフィールを生成する送信者プロフィール生成処理と、

1つ以上の不審メールについての1つ以上の本文データと、前記1つ以上の不審メールについての1つ以上の送信者プロフィールと、が互いに対応付けられた本文一覧ファイルから、前記対象メールの前記送信者プロフィールに対応する本文データを抽出する本文データ抽出処理と、

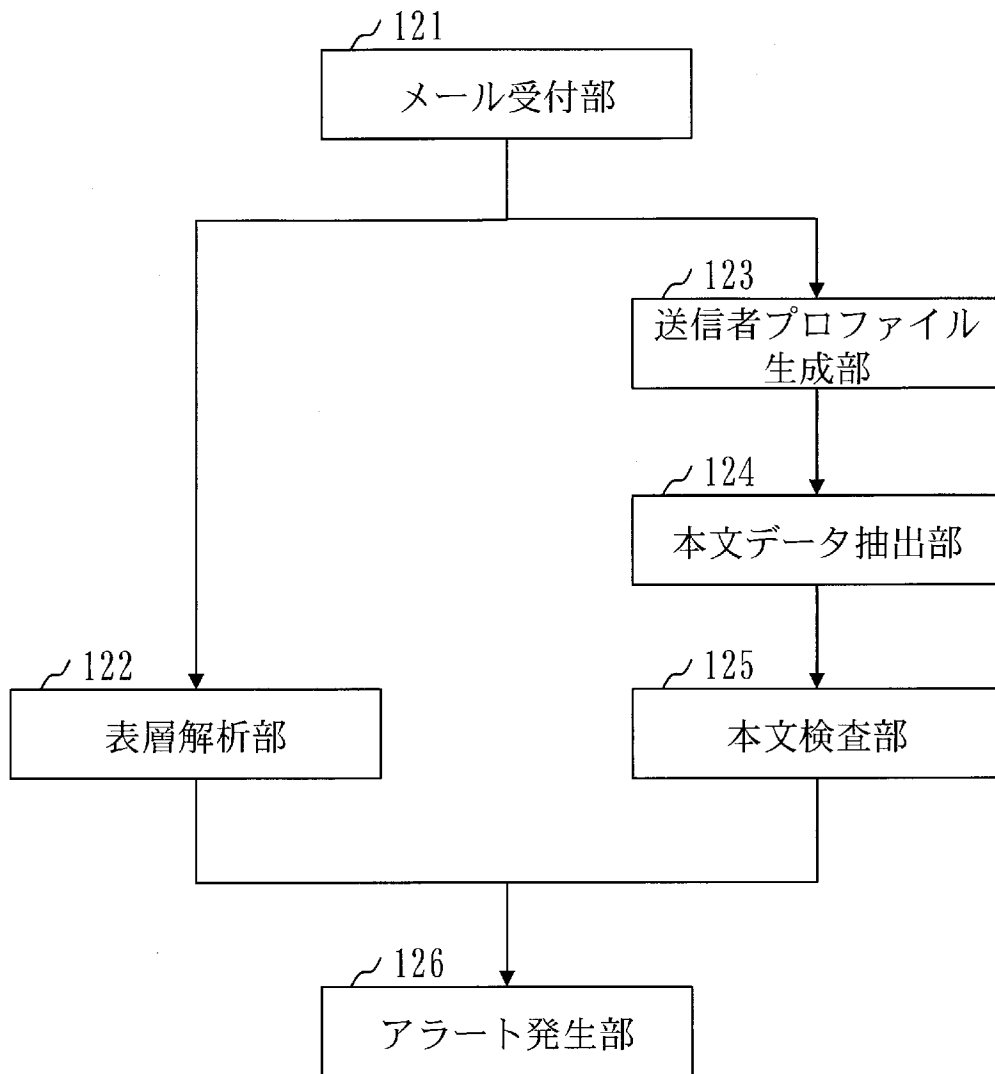
前記対象メールの本文を前記本文一覧ファイルから抽出された本文データと比較し、比較結果に基づいて前記対象メールが不審メールであるか判定する本文検査処理

としてコンピュータを機能させるための不審メール検知プログラム。

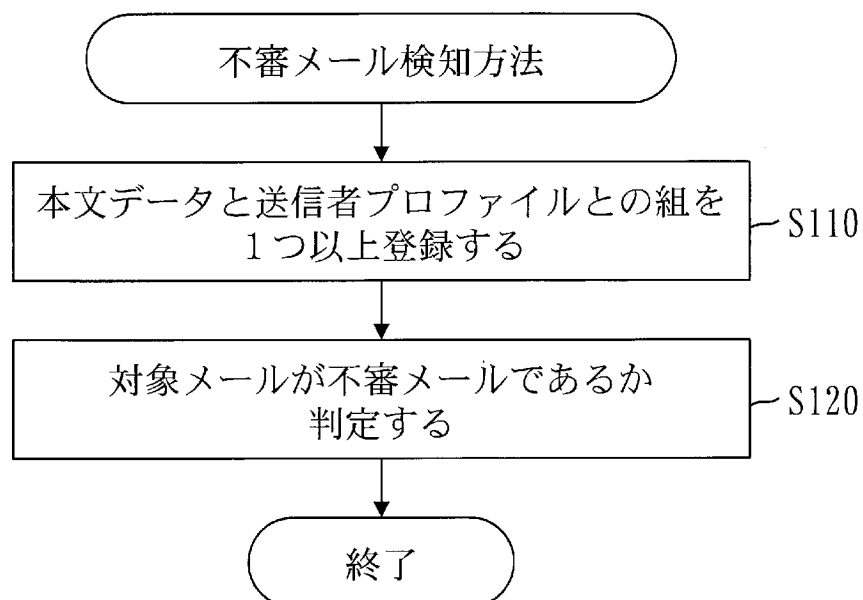
[図1]



[図2]



[図3]



[図4]

131A:本文一覧ファイル
↘

No.	本文データ	送信者プロフィール
1	X ₁ 法人 人事部御中 はじめまして。 私はX ₂ 大学大学院工学研究科のX ₃ と申します。 ...	アドレス：abc@xx.ac.jp, 所属：X ₂ 大学大学院工学研究科, 業界：大学, 属性：学生
2	Y ₁ 社のY ₂ にリモートからコード(命令)が実行 される等の脆弱性が存在します。 ...	アドレス：def@yy.or.jp, 所属：Y ₃ 機構, 業界：IT, 属性：通知
:	:	:

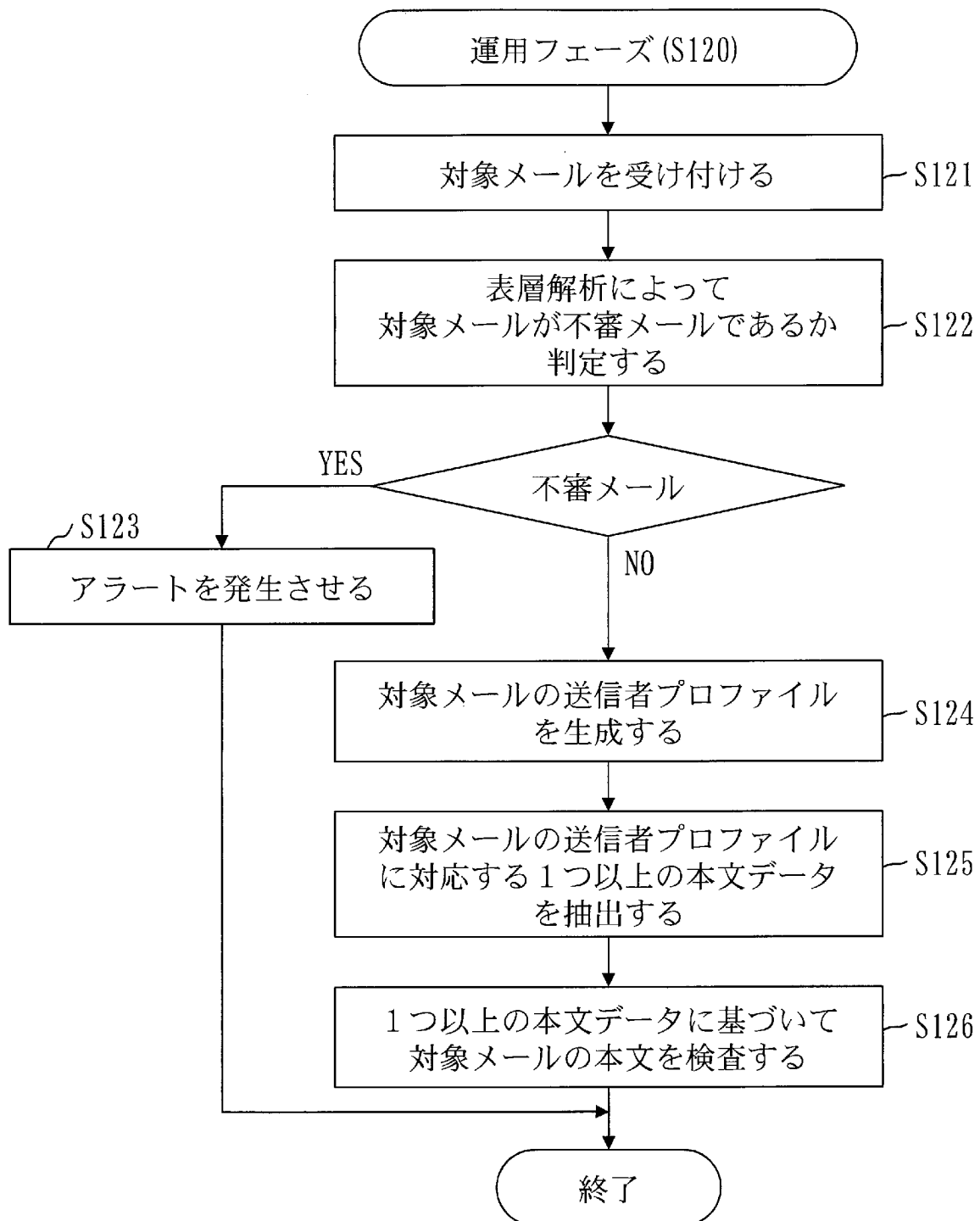
[図5]

131B:本文一覧ファイル

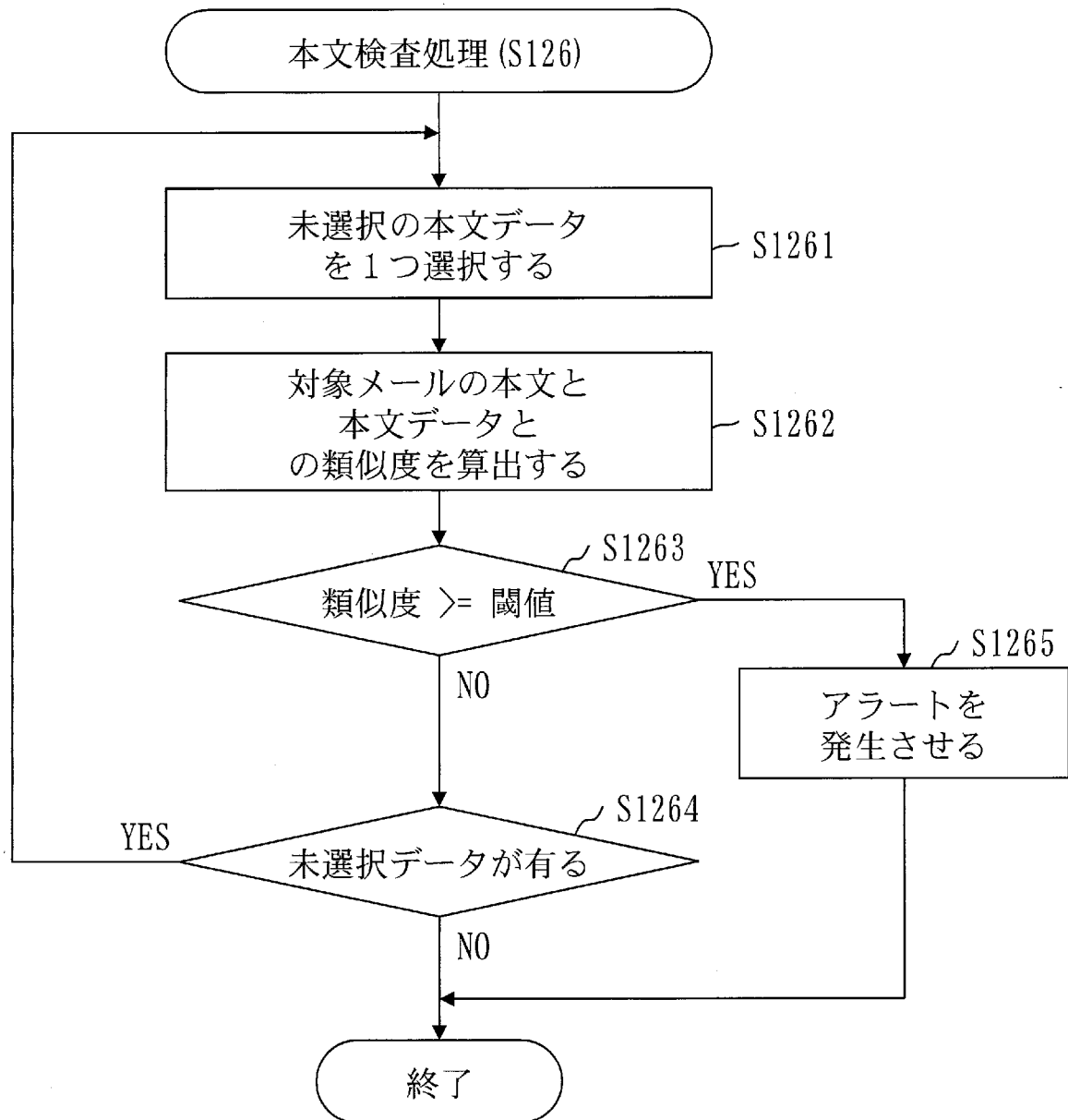


No.	本文データ	送信者プロフィール
1	[組織名], 人事部, 御中, はじめまして, 私, [大学名], 申します	アドレス: abc@xx.ac.jp, 所属: X ₂ 大学院工学研究科, 業界: 大学, 属性: 学生
2	[企業名], [ソフトウェア名], リモート, コード, 命令, 実行, 等, 脆弱性, 存在	アドレス: def@yy.or.jp, 所属: Y ₃ 機構, 業界: IT, 属性: 通知
:	:	:

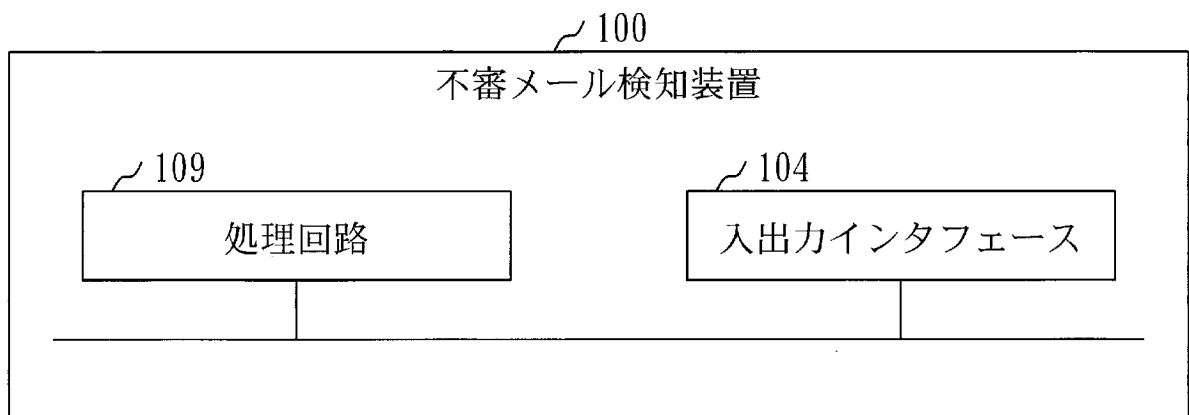
[図6]



[図7]



[図8]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2018/024373

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl. G06F13/00 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl. G06F13/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Published examined utility model applications of Japan 1922-1996

Published unexamined utility model applications of Japan 1971-2018

Registered utility model specifications of Japan 1996-2018

Published registered utility model applications of Japan 1994-2018

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	US 8566938 B1 (ASTRA IDENTITY, INC.) 22 October 2013, column 2, line 50 to column 6, line 26, fig. 1, 2 & US 2016/0014151 A1	1, 4-5 2-3
Y	JP 2012-243146 A (KDDI CORPORATION) 10 December 2012, paragraphs [0041], [0071]-[0081] (Family: none)	2-3

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
13.07.2018

Date of mailing of the international search report
24.07.2018

Name and mailing address of the ISA/
Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl. G06F13/00(2006.01)i

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int.Cl. G06F13/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2018年
日本国実用新案登録公報	1996-2018年
日本国登録実用新案公報	1994-2018年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
X Y	US 8566938 B1 (ASTRA IDENTITY, INC.) 2013.10.22, 第2欄第50行—第6欄第26行, Fig.1-2 & US 2016/0014151 A1	1, 4-5 2-3
Y	JP 2012-243146 A (KDD I 株式会社) 2012.12.10, 段落[0041], [0071]-[0081] (ファミリーなし)	2-3

C欄の続きにも文献が列挙されている。

パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日

13.07.2018

国際調査報告の発送日

24.07.2018

国際調査機関の名称及びあて先

日本国特許庁（ISA/J P）

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）

北川 純次

5 X

3650

電話番号 03-3581-1101 内線 3596